

Garnishment of Accounts Held with Crypto-Asset Service Providers versus Enforcement against Self-Hosted Wallets: Procedural Asymmetries under Romanian Civil Procedure

PhD Student Florentina BIOLAN¹

Abstract

This article examines whether Romanian civil enforcement law can meaningfully distinguish between garnishment of crypto-asset positions held through crypto-asset service providers and enforcement against assets controlled through self-hosted wallets. It combines doctrinal analysis of the Romanian Code of Civil Procedure with contextual interpretation of MiCA, Regulation (EU) 2023/1113, the EBA Travel Rule Guidelines and emerging transnational principles on digital-asset enforcement. The study argues that hosted positions maintained by CASPs can, in principle, be integrated into the traditional logic of third-party garnishment, because the intermediary identifies the client, keeps custody or control-related records and can be ordered to freeze, disclose and transfer attachable positions. By contrast, self-hosted wallets reveal a structural mismatch between classical attachment mechanisms and digital control exercised through private keys. The article concludes that Romanian law already offers a partial basis for enforcement against CASP-held positions, but requires clearer rules on identification, preservation, debtor cooperation, valuation and realisation when assets are held in self-custody.

Keywords: crypto-assets; garnishment; crypto-asset service providers; self-hosted wallets; civil enforcement; Romanian civil procedure.

JEL Classification: K15, K22, K24, K41

DOI: <https://doi.org/10.62768/ADJURIS/2026/6/13>

Please cite this article as:

Biolan, Florentina, „Garnishment of Accounts Held with Crypto-Asset Service Providers versus Enforcement against Self-Hosted Wallets: Procedural Asymmetries under Romanian Civil Procedure,” in *Researching Legal Futures: Towards Transdisciplinary Perspectives on Rights, Technology, and Global Change*, ed. Campina, Ana & Paulo de Brito (Bucharest, Paris, and Calgary: ADJURIS – International Academic Publisher, 2026), 226- 253, <https://doi.org/10.62768/ADJURIS/2026/6/13>.

1. Introduction

1.1. Research Problem and Practical Relevance

The central enforcement question raised by crypto-assets is no longer

¹ Florentina Biolan - Doctoral School of Law, Titu Maiorescu University, Romania. E-mail: biolanflorentina@gmail.com.

whether the legal system can recognise them as economically valuable positions, but whether traditional enforcement techniques can reach them once value is distributed between code, control and intermediation². In this field, the real procedural divide does not run simply between “digital” and “non-digital” assets. It runs, rather, between assets held through a regulated intermediary that may be compelled to cooperate with enforcement authorities and assets controlled directly by the debtor through private credentials, without any legally reachable third party³.

This distinction has become much sharper under the current European regulatory framework. MiCA has transformed CASPs (Crypto-Asset Service Provider) into identifiable professional intermediaries operating within a harmonised authorisation regime, while Regulation (EU) 2023/1113 and the subsequent EBA Travel Rule Guidelines have imposed information duties and, in certain cases, ownership-or-controllership assessments in relation to self-hosted addresses⁴. Yet these instruments, however important for market integrity and AML/CFT compliance, do not by themselves resolve a narrower private-law question: how, exactly, can a creditor or bailiff convert regulatory visibility into effective civil enforcement?

From the viewpoint of Romanian civil procedure, the hosted model offers an immediate point of legal contact. Garnishment may attach sums of money, securities and other attachable intangible movable assets owed to the debtor or held in the debtor’s name by a third party⁵. Once the debtor’s crypto-asset position is maintained through a CASP that provides custody or administration on

² Teresa Rodríguez de las Heras Ballell, “The Emergence of Principles and Best Practices on Digital Assets: Proprietary Rights, and Enforcement,” *European Journal of Risk Regulation*, published online October 4, 2024, 1–12, <https://doi.org/10.1017/err.2024.55>; European Law Institute, *ELI Principles and Guidance for Enforcement Against Digital Assets* (Vienna: European Law Institute, 2025), 1–3, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Projects/Access_to_Digital_Assets/ELI_Principles_and_Guidance_for_Enforcement_Against_Digital_Assets.pdf.

³ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No. 1093/2010 and (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, *Official Journal of the European Union* L 150 (June 9, 2023): 40–205, art. 3(1)(15), art. 149(2), <https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng>.

⁴ Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, *Official Journal of the European Union* L 150 (June 9, 2023): 1–39, recital 58, art. 14(5), art. 16(2), <https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng>; European Banking Authority, *Guidelines on Information Requirements in Relation to Transfers of Funds and Certain Crypto-Assets Transfers under Regulation (EU) 2023/1113 (Travel Rule Guidelines)*, EBA/GL/2024/11 (July 4, 2024), paras. 80–86, <https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-counteracting-financing-terrorism/guidelines-information-requirements-relation-transfers-funds-and-certain-crypto-assets-transfers>.

⁵ Law no. 134/2010 on the Code of Civil Procedure [*Legea nr. 134/2010 privind Codul de procedură civilă*], republished in *Monitorul Oficial al României*, Part I, no. 247 (April 10, 2015), as

behalf of clients, the relationship is no longer purely technical. It becomes a structured legal relationship involving a professional intermediary, an identifiable client position and, potentially, a patrimonial entitlement that may be frozen, disclosed, validated and realised through procedures functionally comparable to third-party garnishment.⁶

The self-hosted model produces a radically different procedural landscape. Where the debtor controls the asset through a private key or analogous means of access, no intermediary holds the position in the debtor's name and no institution can be served as a classic garnishee. Even when blockchain data points to a relevant address, enforcement still faces three cumulative obstacles: attribution, coercion and preservation.⁷ The creditor must first connect the address to the debtor with a satisfactory evidentiary standard; must then determine whether and to what extent the debtor may be compelled to cooperate; and must finally preserve and realise the asset without destroying the very means through which control is exercised. In this context, "control" displaces physical possession as the practical category around which enforcement must be reorganised.⁸

The problem investigated in this article is therefore not whether crypto-assets can be treated, in the abstract, as patrimonial values. The real issue is whether current Romanian civil procedure adequately differentiates between two legally distinct holding models: intermediary-based custody and direct self-custody.⁹ This distinction matters because a creditor's realistic chances of recovery depend less on the digital nature of the asset than on the architecture through which legal and factual control over that asset is exercised.

1.2. Novelty, Methodology, Structure and Working Hypothesis

The novelty of the present study lies in shifting the focus away from the now familiar public-law themes of crypto regulation, AML/CFT compliance or

subsequently amended, art. 781(1), art. 787(1), art. 790(1), art. 792(1)–(2), art. 793, <https://legislatie.just.ro/Public/DetaliiDocument/140271>.

⁶ Regulation (EU) 2023/1114, art. 3(1)(16)(a), art. 75(1), (6)–(8); Dirk Zetzsche and Jannik Woxholth, "Crypto Custody," in *The EU Law on Crypto-Assets: A Guide to European FinTech Regulation* (Cambridge: Cambridge University Press, 2025), 130–143, <https://doi.org/10.1017/9781009196338.010>.

⁷ Matthias Lehmann, "Who Owns Bitcoin? Private Law Facing the Blockchain," *Minnesota Journal of Law, Science & Technology* 21, no. 1 (2020): 93–136, <https://doi.org/10.24926/15529541.3823>.

⁸ European Law Institute, *ELI Principles and Guidance*; Christian Koller and Matthias Lehmann, eds., *Digital Assets in Enforcement and Insolvency: Securing Creditor Access and Protecting Customer Interests in the Crypto World* (Oxford: Hart Publishing, 2025), <https://doi.org/10.5040/9781509976782>.

⁹ Dirk Zetzsche and Jannik Woxholth, "Private Law of Cryptoassets," in *The EU Law on Crypto-Assets: A Guide to European FinTech Regulation* (Cambridge: Cambridge University Press, 2025), 203–216, <https://doi.org/10.1017/9781009196338.015>.

the general legal classification of blockchain-based assets, and towards the mechanics of enforcement itself.¹⁰ Existing doctrinal approaches have extensively examined the legal nature of crypto-assets, the regulation of CASPs, the implications of custody, the role of private law and the harmonising function of transnational principles. Far fewer analyses, especially from the perspective of Romanian civil procedure, have isolated the procedural asymmetry between garnishment of CASP-held positions and enforcement against self-hosted wallets as a standalone research problem.¹¹

Methodologically, the article combines doctrinal analysis of Romanian positive law with a functional and teleological reading of the applicable European framework. The rules on garnishment in the Romanian Code of Civil Procedure are interpreted together with MiCA's provisions on CASP authorisation and custody, the information architecture of Regulation (EU) 2023/1113, the EBA Travel Rule Guidelines and the recent transnational guidance developed for enforcement against digital assets. The research proceeds from a simple but operational hypothesis: in the field of digital assets, enforceability is shaped primarily by the existence of legally reachable intermediation, not by the mere fact that the asset exists on a distributed ledger.

The structure of the paper follows that hypothesis. Section 2 sets out the normative and conceptual premises, distinguishing hosted accounts from self-hosted wallets in legally relevant terms. Section 3 analyses the garnishment of accounts held with CASPs under Romanian civil procedure and tests whether the CASP can function as a third-party garnishee. Section 4 addresses enforcement against self-hosted wallets and identifies the limits of classical attachment where no intermediary can be bound. Section 5 develops a functional comparison between the two models, with particular attention to evidentiary asymmetry, procedural efficiency and debtor protection. Section 6 formulates *de lege lata* and *de lege ferenda* observations. The conclusion defended throughout the article is that Romanian law already contains a partial framework for adapting garnishment to CASP-held positions, whereas self-hosted wallets reveal a structural enforcement gap that cannot be overcome by simple analogy with bank-account garnishment.

¹⁰ Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Cambridge, MA: Harvard University Press, 2018), <https://doi.org/10.4159/9780674985933>; Kevin Werbach, *The Blockchain and the New Architecture of Trust* (Cambridge, MA: MIT Press, 2018), <https://doi.org/10.7551/mitpress/11449.001.0001>; Chris Brummer, ed., *Cryptoassets: Legal, Regulatory, and Monetary Perspectives* (New York: Oxford University Press, 2019), <https://doi.org/10.1093/oso/9780190077310.001.0001>.

¹¹ Rodríguez de las Heras Ballell, "Emergence of Principles and Best Practices"; Koller and Lehmann, *Digital Assets in Enforcement and Insolvency*.

2. Normative and Conceptual Premises

2.1. CASPs as Professional Intermediaries under MiCA

Under MiCA, a crypto-asset service provider is not merely a technical facilitator operating at the margins of digital markets, but a legal person or other undertaking whose business consists in providing one or more crypto-asset services to clients on a professional basis.¹² This requalification is decisive for private law analysis. Once crypto-assets are held through a CASP, the relationship between user and infrastructure is no longer exhausted by code or by unilateral control over a distributed ledger address. It is mediated through an identifiable professional operator, subject to authorisation, supervision and conduct-of-business duties. In legal terms, the hosted environment thus transforms a seemingly disintermediated asset into a position embedded in an institutional relationship.

The point becomes even clearer in relation to custody and administration. MiCA defines that service as the safekeeping or controlling, on behalf of clients, of crypto-assets or of the means of access to such crypto-assets, including, where applicable, private cryptographic keys.¹³ Article 75 then imposes a dense matrix of obligations on the provider: a contractual framework specifying responsibilities, periodic statements of position, procedures enabling the return of the assets or of the means of access, segregation of client holdings from proprietary holdings, and liability for loss attributable to the provider. From the standpoint of enforcement law, these obligations are relevant not only as investor-protection tools, but also as mechanisms that produce legal visibility. They presuppose that the provider can identify the client's position, distinguish it from its own estate and operationally react to a demand affecting that position.

The hosted model is reinforced by Regulation (EU) 2023/1113. That regulation deliberately aligns its terminology with MiCA and assumes that the CASP of the originator and the CASP of the beneficiary are capable of collecting, retaining and transmitting identifying information linked to a transfer.¹⁴ In conceptual terms, this confirms that a CASP is not just an interface through which clients interact with a blockchain network. It is a professional intermediary located between the client and the transactional infrastructure, capable of maintaining account information, attributing transfers to a client relationship and responding to legally relevant requests. This institutional layer is precisely what makes hosted

¹² Regulation (EU) 2023/1114, art. 1(2)(b), art. 3(1)(15)–(16), art. 59; Dirk Zetzsche and Jannik Woxholth, *The EU Law on Crypto-Assets: A Guide to European FinTech Regulation* (Cambridge: Cambridge University Press, 2025), <https://doi.org/10.1017/9781009196338>.

¹³ Regulation (EU) 2023/1114, art. 3(1)(17), art. 75(1), (5)–(8); Zetzsche and Woxholth, *EU Law on Crypto-Assets*.

¹⁴ Regulation (EU) 2023/1113, recital 38, recital 39, art. 3(15), art. 3(19), art. 14–16; European Banking Authority, *Travel Rule Guidelines*, paras. 77–87.

crypto-asset positions structurally comparable, though not identical, to other intermediary-held intangible assets already familiar to enforcement law.

2.2. Self-Hosted Wallets and the Legal Relevance of Exclusive Control over Private Keys

By contrast, the expression “self-hosted wallet,” commonly used in practice, refers in legal terms to the use of a self-hosted address, namely a distributed ledger address not linked either to a CASP or to a non-Union entity providing similar services.¹⁵ Regulation (EU) 2023/1113 also distinguishes person-to-person transfers of crypto-assets, meaning transfers carried out without the involvement of any CASP. For enforcement purposes, the crucial point is therefore not the informal word *wallet* as such, but the structural absence of a professional intermediary standing between the user and the digital asset. What matters is that the address from which the transfer is initiated is not institutionally embedded in an account relationship managed by a regulated third party.

The legal significance of self-hosting becomes even sharper if MiCA’s definition of custody is read inversely. If custody and administration exist where a third party safeguards or controls the crypto-assets, or the means of access to them, on behalf of the client, the self-hosted scenario is the opposite situation: the means of access remain under the user’s own control.¹⁶ In the digital-asset environment, this control should not be collapsed into the language of physical possession. It is, rather, a technologically mediated power of exclusion and disposition: the person controlling the relevant private key, seed phrase or equivalent access mechanism is, in functional terms, the person able to initiate transfers, prevent others from using the asset and capture its economic value. It is no coincidence that recent transnational work on digital assets has placed the category of control at the center of legal analysis, precisely because corporeal possession does not adequately describe how these assets are held and transferred.

This does not mean that self-hosted positions are wholly opaque in law. Once a transfer to or from a self-hosted address interacts with a CASP, Union law requires the provider to obtain and hold relevant information and, where the amount exceeds EUR 1,000, to assess whether that address is owned or controlled by the relevant customer.¹⁷ The EBA Travel Rule Guidelines further operationalise this obligation by indicating that CASPs may rely on technical methods such as blockchain analytics, customer-supplied information, micro-transfers, digital signature checks or combinations of such methods. The conceptual consequence

¹⁵ Regulation (EU) 2023/1113, art. 3(20), recital 38, recital 39.

¹⁶ Regulation (EU) 2023/1114, art. 3(1)(17); European Law Institute, *ELI Principles and Guidance*; Rodríguez de las Heras Ballell, “Emergence of Principles and Best Practices.”

¹⁷ Regulation (EU) 2023/1113, art. 14(5), art. 16(2); European Banking Authority, *Travel Rule Guidelines*, paras. 77–87.

is important: self-custody is not erased by regulation, but only partially translated into evidence when the asset touches a regulated gateway. Outside that gateway, the concentration of control at user level remains intact.

2.3. Why the Hosted/Self-Hosted Distinction Matters for Enforcement Law

For enforcement law, the hosted/self-hosted distinction is decisive because classical garnishment relies on a triangular procedural structure: creditor, debtor and a third party that owes attachable claims to the debtor or holds attachable intangible assets in the debtor's name. Romanian civil procedure expressly allows garnishment over sums of money, securities and other attachable intangible movable assets owed to the debtor or held in the debtor's name by a third person.¹⁸ A crypto-asset position maintained through a CASP can, at least at a functional level, be examined within this architecture, because there is an identifiable intermediary that may freeze, disclose, preserve or ultimately enable the realisation of the debtor's position. The hosted model therefore creates an enforcement contact point that the self-hosted model lacks.

The self-hosted model destabilises that logic at each stage. First, there may be no third-party garnishee against whom an order can be directed. Second, attribution becomes significantly more difficult, because the creditor must link a given address, or a cluster of addresses, to the debtor with a sufficiently persuasive evidentiary basis. Third, preservation is no longer a matter of addressing a third party and waiting for institutional compliance; it becomes a question of whether the debtor can be compelled to cooperate and whether the relevant access credentials can be secured without compromising the asset itself. This is why the emerging European guidance on enforcement against digital assets pays particular attention to disclosure obligations, search measures, access to digital assets, seizure techniques, valuation and realisation¹⁹.

The deeper implication is that the decisive dividing line is not the abstract opposition between "traditional assets" and "digital assets," but the more precise distinction between intermediated control and direct control.²⁰ Hosted accounts externalise control into an institutional relationship and therefore permit, even if

¹⁸ Law no. 134/2010 on the Code of Civil Procedure, art. 781(1), art. 787, art. 792, art. 793; Regulation (EU) 2023/1114, art. 75.

¹⁹ European Law Institute, *ELI Principles and Guidance*; Koller and Lehmann, *Digital Assets in Enforcement and Insolvency*.

²⁰ Rodríguez de las Heras Ballell, "Emergence of Principles and Best Practices"; Anna Veneziano and Teresa Rodríguez de las Heras Ballell, "Digital Assets in Insolvency and Enforcement Proceedings: Some Insights from UNIDROIT's Work," in *Digital Assets in Enforcement and Insolvency: Securing Creditor Access and Protecting Customer Interests in the Crypto World*, ed. Christian Koller and Matthias Lehmann (Oxford: Hart Publishing, 2025), 27–43, <https://doi.org/10.5040/9781509976782>.

imperfectly, the adaptation of classical enforcement techniques. Self-hosted wallets internalise control at debtor level and reveal a structural gap in procedures originally built for assets that are either physically locatable or institutionally intermediated. For that reason, the hosted/self-hosted distinction must be treated as a threshold analytical criterion, not as a merely descriptive or technological one.

Seen in this light, the distinction is not semantic. It determines the object of attachment, the addressee of enforcement measures, the evidentiary route open to the creditor and the techniques through which value may ultimately be preserved and realised.²¹

3. Garnishment of Accounts Held with CASPs under Romanian Civil Procedure

3.1. The Legal Qualification of the Debtor's Position vis-à-vis the CASP

The starting point of the analysis is that a creditor does not garnish “the blockchain” in the abstract, nor does Romanian civil procedure need to resolve, at the outset, every theoretical controversy concerning the ontological status of crypto-assets. In the hosted environment, the immediate object of enforcement is the debtor's patrimonial position vis-à-vis an identifiable intermediary. Once a CASP provides custody and administration on behalf of a client, the relevant legal relationship is no longer exhausted by the debtor's factual ability to interact with a distributed ledger address. It becomes a structured legal relationship in which the intermediary keeps records, attributes positions to a client, and is under a duty to return crypto-assets or the means of access to them.²²

This is sufficient, in principle, to bring the hosted position within the logic of Romanian garnishment law. Article 781 of the Code of Civil Procedure does not limit garnishment to classic bank deposits or narrowly defined receivables. It extends to sums of money, securities and other attachable intangible movable assets owed to the debtor or held in the debtor's name by a third party, including future sums or claims arising from existing legal relationships.²³ Read functionally, this formula is broad enough to capture an individualised crypto-asset position maintained by a CASP, even if doctrinal opinion continues to oscillate between proprietary, obligational or hybrid explanations of the client's entitlement.

²¹ Koller and Lehmann, *Digital Assets in Enforcement and Insolvency*; European Law Institute, *ELI Principles and Guidance*.

²² Regulation (EU) 2023/1114, art. 3(1)(16)–(17), art. 75(1), (5)–(8); Zetzsche and Woxholth, *EU Law on Crypto-Assets*.

²³ Law no. 134/2010 on the Code of Civil Procedure, art. 781(1), (4); Lehmann, “Who Owns Bitcoin?”

In the case of custody and administration, the debtor's position should therefore be qualified, for enforcement purposes, at least as an attachable claim to return the crypto-assets held on the client's behalf or, where relevant, the means of access to those assets. MiCA strongly supports that conclusion. It requires the provider to maintain a contractual framework, record the client's positions, issue periodic statements, ensure return procedures, segregate client holdings from its own estate and bear liability for certain losses attributable to it.²⁴ These elements do not eliminate all private-law debate, but they do make one point sufficiently clear for enforcement law: the debtor has an economically and legally individualised position against the CASP, and that position is capable of being frozen and, where appropriate, realised.

The qualification may, however, vary according to the specific service provided. If the relevant CASP relationship concerns not custody but exchange, execution of orders or reception and transmission of orders, the attachable object may be narrower. In such cases, the creditor may be targeting fiat balances, settlement proceeds, temporary claims arising from an executed order or another intermediary-held patrimonial position, rather than crypto-assets continuously held in custody by the provider.²⁵ Not every interaction with a CASP should therefore be treated as equivalent to a custodial account. The legal qualification of the debtor's position must follow the concrete service architecture, not the mere fact that the debtor uses a crypto platform.

3.2. The CASP as a Third-Party Garnishee

Once the debtor's hosted position is understood as an attachable patrimonial entitlement against an intermediary, the next step is to determine whether the CASP can operate, under Romanian law, as a third-party garnishee. The answer should, in principle, be affirmative. Romanian civil procedure establishes garnishment without prior summons, by service of the garnishment order on the third party identified under Article 781, while the debtor is then informed of the measure taken. From that moment, the third party is prohibited from making payments or carrying out operations that would diminish the attached assets.²⁶ A CASP holding crypto-assets or related balances in the debtor's name falls, functionally, within that triangular structure.

This conclusion is reinforced by MiCA's institutional architecture. A

²⁴ Regulation (EU) 2023/1114, art. 75(5)–(8); Rodríguez de las Heras Ballell, “Emergence of Principles and Best Practices.”

²⁵ Regulation (EU) 2023/1114, art. 3(1)(16), arts. 79–80; Law no. 134/2010 on the Code of Civil Procedure, art. 781(1); Zetsche and Woxholth, *EU Law on Crypto-Assets*.

²⁶ Law no. 134/2010 on the Code of Civil Procedure, art. 783(1)–(2), art. 784(1)–(4); Regulation (EU) 2023/1114, art. 75(5)–(7).

CASP is not an informal technological actor but a professional intermediary subject to authorisation, record-keeping duties, business continuity requirements and client-facing obligations. MiCA requires position statements, record retention, segregation procedures and operational arrangements ensuring the continuity of services. In addition, when authorisation is withdrawn, the provider must maintain procedures for the timely and orderly transfer of clients' crypto-assets and funds to another CASP.²⁷ These obligations show that the hosted position is administratively knowable and operationally controllable by the intermediary. From an enforcement perspective, that is exactly what makes a CASP a plausible addressee of a garnishment order.

The procedural status of the CASP should nevertheless not be overstated. Romanian law does not transform the garnishee into a substitute debtor in all respects from the outset. The CASP becomes the addressee of freezing and compliance duties, but the legal correctness of the attachment may still be litigated if validation becomes necessary. This is important because Article 787(5) of the Code of Civil Procedure bars the third-party garnishee from challenging the garnishment itself by way of an independent objection, yet Article 790 allows the garnishee, within validation proceedings, to raise against the attaching creditor the substantive defences it could have raised against the debtor, so far as those defences are based on causes predating the garnishment.²⁸ For CASPs, that procedural balance is significant: it prevents purely dilatory resistance, while preserving the possibility of showing, for example, that the relevant position does not exist, is not due, has already been extinguished or is not attributable to the debtor identified in the enforcement file.

3.3. Procedural Effects of Garnishment: Freezing, Disclosure, Preservation and Liquidation

The first and most immediate effect of garnishment is freezing. Under Article 784 of the Code of Civil Procedure, all attached sums and assets become unavailable from the moment the garnishment order is communicated to the third-party garnishee; that unavailability extends, where applicable, to future sums, civil fruits and accessories, and renders subsequent dispositions ineffective against the attaching creditor.²⁹ In the context of a hosted crypto account, the legal meaning of freezing should be understood in technologically adapted terms. It should prevent outbound withdrawals, internal transfers to other user accounts, conversion into fiat or other crypto-assets, and any operational step that would

²⁷ Regulation (EU) 2023/1114, art. 59(2), (7), art. 64(8), art. 68(7)–(9), art. 75(5)–(7); Zetzsche and Woxholth, *EU Law on Crypto-Assets*.

²⁸ Law no. 134/2010 on the Code of Civil Procedure, art. 787(5), art. 790(1)–(4), art. 792(1)–(3).

²⁹ Law no. 134/2010 on the Code of Civil Procedure, art. 784(1)–(4), art. 787(1), (3), art. 790(3), (7)–(9); European Law Institute, *ELI Principles and Guidance*, principles 7–8.

reduce or alter the attached position to the creditor's detriment. The underlying idea is classical, even if the operational forms are new: once the intermediary has been served, the debtor must no longer be able to dissipate the garnished value through that intermediary.

Disclosure is the second major effect, although Romanian law does not yet articulate it in crypto-specific detail. *De lege lata*, the CASP must at least react in a manner that makes the garnishment effective: it must identify whether it owes funds or holds attachable intangible assets for the debtor, preserve those assets, and provide the executor with proof of compliance. Where validation proceedings are brought, the court may order any evidence necessary to determine whether the third party actually owes or holds attachable value for the debtor.³⁰ In practice, a meaningful crypto-sensitive disclosure should include, at minimum, identification of the relevant account relationship, the type of assets held, the balance or quantity, the approximate value at the relevant time, the existence of pending settlement operations and the existence of prior attachments or other restrictions. Emerging European guidance on enforcement against digital assets confirms that, without reliable disclosure by custodians and service providers, enforcement becomes uncertain even where the law recognises the asset as enforceable.³¹

Preservation is the third effect and, in the hosted model, it is the point at which CASP-based enforcement shows its greatest advantage over self-custody. MiCA requires custody providers to segregate client holdings from their own estate, to keep the means of access clearly identified and to ensure the return of the crypto-assets or access means to the client as soon as possible when required. It also requires continuity arrangements and, in the event of withdrawal of authorisation, procedures ensuring the timely and orderly transfer of client assets and funds to another CASP.³² These duties do not eliminate all operational risk, but they materially reduce the chance that the attached position will disappear merely because the intermediary is disorganised or because its own creditors intervene. They also matter for the scope of attachment: where a protocol change or other event modifies the client's rights, MiCA entitles the client, in principle, to the newly created crypto-assets or rights corresponding to the client's position at the relevant time, unless the contract validly provides otherwise.³³ For enforcement purposes, this suggests that the attached hosted position may include not only the frozen balance strictly viewed at the moment of service, but also derivative rights generated by that position during the freeze period, insofar as those rights accrue

³⁰ Law no. 134/2010 on the Code of Civil Procedure, art. 787(5), art. 790(1)–(4), art. 792(1)–(3).

³¹ Law no. 134/2010 on the Code of Civil Procedure, art. 784(1)–(4), art. 787(1), (3), art. 790(3), (7)–(9); European Law Institute, *ELI Principles and Guidance*, principles 7–8.

³² Regulation (EU) 2023/1114.

³³ Regulation (EU) 2023/1114, art. 75(4)–(7); European Law Institute, *ELI Principles and Guidance*, principle 10; Koller and Lehmann, *Digital Assets in Enforcement and Insolvency*.

to the debtor under the governing contractual and regulatory framework.

Liquidation is the final stage and also the one at which analogy with bank-account garnishment becomes most fragile. Where the garnishee fails to comply, Articles 790 and 792 of the Code of Civil Procedure allow validation; once the validation decision becomes final, it operates as an assignment of the claim and constitutes an enforceable title against the garnishee. If the attachment concerns securities or other intangible movable assets, Article 793 of the Code of Civil Procedure provides that the enforcement officer shall realise them according to the rules governing movable enforcement, while also taking into account any special rules applicable to those assets.³⁴ In the case of crypto-assets held with a CASP, this strongly suggests that liquidation should follow a staged approach: identification of the asset, preservation of control, valuation, and then realisation by an appropriate method. Automatic conversion by the CASP should not simply be presumed. The Code of Civil Procedure expressly authorises certain unilateral currency conversions for bank accounts, but it does not establish an equivalent automatic rule for crypto-assets. Given price volatility and the diversity of market venues, the safer view is that liquidation should occur only within the framework of a properly instructed or judicially supervised realisation process. The ELI Principles are instructive here: they recommend that valuation and realisation methods be adapted to volatility, pricing uncertainty and market structure, and that market price be used where a recognised market exists, while reasonable steps should otherwise be taken to maximise realisation value.

3.4. Cross-Border and Practical Obstacles

The legal plausibility of CASP garnishment does not mean that it is frictionless in practice. The first difficulty is cross-border service provision. MiCA allows authorised CASPs to provide services throughout the Union either through establishment or through the freedom to provide services, and expressly states that a CASP providing cross-border services need not have a physical presence in the host Member State. Article 65 then sets up a home-state notification mechanism for service provision in additional Member States.³⁵ For a Romanian creditor, this means that the debtor may use a CASP lawfully serving the Romanian market from another Member State without any Romanian branch. In regulatory terms, that is unremarkable; in enforcement terms, it complicates the identification of the operational addressee, the language of communication, the speed of compliance and the practical follow-up if the provider reacts partially or ambiguously.

The problem is even more acute where the relevant platform is a third-

³⁴ Law no. 134/2010 on the Code of Civil Procedure, art. 784(7)–(8), art. 790(4)–(8), art. 792(1)–(2), art. 793; European Law Institute, *ELI Principles and Guidance*, principle 10.

³⁵ Regulation (EU) 2023/1114, art. 59(7), art. 65(1)–(4).

country firm. MiCA permits, under Article 61, the provision of services at the exclusive initiative of a Union client without full Union authorisation. Whatever its regulatory justification, that mechanism weakens the enforcement advantages associated with the hosted model, because the creditor may be dealing with an intermediary that is outside the normal authorisation and supervisory architecture on which intra-Union visibility and cooperation are built.³⁶ In such a situation, garnishment may remain theoretically possible, but the practical leverage of Romanian enforcement organs is diminished, especially where there is no EU establishment, no host-state operational point of contact and no reliable path for rapid operational compliance.

A second group of obstacles concerns the internal complexity of the hosted position itself. Although MiCA considerably improves legal visibility, the enforcement file still has to determine which service is being used, whether the relevant position is immediately realisable, whether it is already subject to restrictions, and what exactly counts as the garnished value at a given moment. Volatility affects valuation; token-specific mechanics may affect transferability; and protocol events may create incidental rights during the enforcement period. MiCA's rule that rights newly created by an underlying protocol event accrue to the client according to the client's position at the relevant time illustrates why a CASP-held balance is not always a static number. In addition, the more dynamic the account activity, the greater the risk of mismatch between the legal moment of indisponibilisation and the operational moment at which the intermediary actually prevents outgoing activity.

For these reasons, the hosted model should not be romanticised. It is clearly more compatible with Romanian garnishment law than self-custody, because it supplies an identifiable third party and a documentary trail. Yet it still requires careful adaptation in relation to service architecture, account mapping, valuation, market timing and cross-border execution. The proper conclusion is therefore not that a CASP account is simply the digital equivalent of a bank account, but that it is an attachable intermediary-held position whose enforcement is legally feasible under current Romanian law, albeit only through a technologically informed reading of classical garnishment rules.³⁷

³⁶ Regulation (EU) 2023/1114, art. 61(1)–(3).

³⁷ Regulation (EU) 2023/1114, art. 75(4)–(7); European Law Institute, *ELI Principles and Guidance*, principle 10; Rodríguez de las Heras Ballell, “Emergence of Principles and Best Practices.”

4. Enforcement Against Self-Hosted Wallets: The Limits of Classical Attachment

4.1. The Object of Enforcement and the Challenge of Legal Characterisation

In the self-hosted environment, the first difficulty is conceptual. The enforceable object is not the wallet application, browser extension, or hardware device as such, but the digital asset position recorded on the relevant ledger and economically controlled through the credentials linked to that position.³⁸ The legal vocabulary of “wallet” is convenient yet imprecise: it may refer to software, hardware, an interface, a set of addresses, or merely a means of interacting with a distributed ledger. For enforcement purposes, that distinction matters because the device or software may be seized as evidentiary support, while the asset itself remains an incorporeal value existing independently of the interface through which it is accessed.³⁹

Romanian civil procedure does not exclude such assets from the sphere of enforcement, but it does not offer an express crypto-specific category either. Article 781 of the Code of Civil Procedure is built around attachment by garnishment of claims, sums of money, securities and other attachable intangible movables owed by, or held in the name of the debtor by, a third party.⁴⁰ That model is structurally ill-suited to self-hosted wallets because no intermediary stands between debtor and asset. The decisive procedural difficulty is therefore not the patrimonial value of the digital asset, but the absence of the classic garnishee on whom freezing and compliance duties can be imposed.

This is why the concept of control is more useful than the borrowed language of possession. The UNIDROIT Principles treat control of a digital asset as a functional equivalent of possession, while the ELI Principles define access to digital assets by reference to the possibility of actual attachment and effective seizure.⁴¹ In self-custody, the object of enforcement is best described as the debtor’s control-enabled digital asset position. By contrast, the seed phrase, private key, hardware wallet or backup file are not the asset itself, but the practical means through which enforcement may or may not obtain dominion over that

³⁸ Regulation (EU) 2023/1113, art. 3, art. 14(5), art. 16(2).

³⁹ Lehmann, “Who Owns Bitcoin?”; Louise Gullifer and Ignacio Tirado, “Proprietary Rights and Digital Assets: A ‘Modest Proposal’ from a Transnational Law Perspective,” *Law and Contemporary Problems* 87, no. 2 (2025): 211–232, <https://scholarship.law.duke.edu/lcp/vol87/iss2/9/>.

⁴⁰ Law no. 134/2010 on the Code of Civil Procedure, art. 781(1).

⁴¹ UNIDROIT, *Principles on Digital Assets and Private Law* (Rome: UNIDROIT, 2023), principle 6 and commentary 6.6, <https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/>; European Law Institute, *ELI Principles and Guidance*, principle 8.

asset.⁴²

4.2. Identifying the Wallet and Proving the Debtor's Control

Once the object of enforcement is properly characterised, the next obstacle is evidentiary. Regulation (EU) 2023/1113 and the EBA Travel Rule Guidelines themselves distinguish between identifying whether the other end of a transfer is a self-hosted address and establishing whether that address is owned or controlled by the relevant person.⁴³ This distinction is crucial in civil enforcement. An address may be visible on-chain without being attributable to the debtor, and it may be historically linked to the debtor without sufficient proof that the debtor still controls it at the moment enforcement is sought.

The EBA Guidelines are instructive because they set out a concrete menu of verification techniques: blockchain analytics, third-party data providers, direct information obtained from the customer, unattended or attended remote verification, the sending of a minimal predefined transfer, digital signature of a specified message and other suitable technical means.⁴⁴ Although these methods were designed for AML/CFT compliance rather than for civil execution, they are highly relevant from a probative standpoint. They show that proof of control in the digital environment is rarely reducible to a single evidentiary act; it is ordinarily the result of a cumulative assessment built from technical traces, transactional history and demonstrable ability to operate the relevant address.

Under Romanian law, this means that proof should be assembled as a composite evidentiary package. Article 790 of the Code of Civil Procedure already allows the court, in validation proceedings, to take any evidence admissible under ordinary law.⁴⁵ By analogy, where the creditor seeks judicial measures concerning self-hosted assets, the file may need to combine on-chain tracing, records from prior CASP interactions, KYC (Know Your Customer) documentation, device examinations, debtor statements, communications and expert reports. A historical transfer from a known exchange account to a given address should therefore be treated as an evidentiary lead, not as conclusive proof of present control.⁴⁶

Technical expertise becomes indispensable at this stage. The ELI Principles expressly state that search measures and access to information should be proportionate and effective and envisage the use of computer experts where the

⁴² Regulation (EU) 2023/1114, art. 3(1)(17).

⁴³ Regulation (EU) 2023/1113, art. 14(5), art. 16(2); European Banking Authority, *Travel Rule Guidelines*, paras. 77–79.

⁴⁴ European Banking Authority, *Travel Rule Guidelines*, paras. 83–86.

⁴⁵ Law no. 134/2010 on the Code of Civil Procedure, art. 790(3).

⁴⁶ UNIDROIT, *Principles on Digital Assets and Private Law*, principle 6 and commentary 6.6; Rodríguez de las Heras Ballell, “Emergence of Principles and Best Practices.”

enforcement agent lacks the technical knowledge necessary to identify digital assets.⁴⁷ In practice, the decisive question is rarely whether a wallet exists, but whether a properly documented chain of evidence can persuade the court that the debtor presently retains operational control over it.

4.3. Debtor Cooperation, Disclosure Orders and Procedural Limits

In the absence of a reachable intermediary, enforcement against self-hosted wallets depends far more heavily on debtor cooperation. Effective execution may require disclosure of addresses, wallet software, device locations, backup arrangements, multisignature participation, recovery phrases or other access-related information.⁴⁸ The ELI Principles treat debtor and third-party cooperation as a core precondition of meaningful enforcement and warn that a lack of cooperation can render enforcement structurally ineffective.

Yet cooperation cannot be conceived in overly abstract or absolute terms. A request to identify a relevant address is not equivalent to an order requiring the debtor to surrender all credentials or to sign an irreversible transfer transaction. Because private keys and seed phrases may unlock entire clusters of assets, including assets that are not subject to enforcement or assets held jointly or on behalf of others, overbroad orders raise acute issues of proportionality, confidentiality and cybersecurity.⁴⁹ The functional centrality of control in digital-asset law is precisely why access orders must be narrowly tailored.

From a Romanian *de lege lata* perspective, the current Code of Civil Procedure does not expressly regulate a crypto-specific mechanism compelling the debtor to reveal a seed phrase, to digitally sign a message, or to execute an on-chain transfer under the supervision of the enforcement officer.⁵⁰ This is an inference from the present text of the Code of Civil Procedure, which contains general rules on garnishment, validation and realisation of attachable assets but no tailored rule on access to debtor-controlled digital assets. The result is a zone of procedural uncertainty: courts may be inclined to rely on analogy and general enforcement logic, but the legal basis for intrusive access measures remains insufficiently articulated.

For that reason, any search or disclosure measure directed at self-hosted wallets should be justified by necessity and calibrated by proportionality. The ELI Principles recommend that mechanisms for obtaining information and

⁴⁷ European Law Institute, *ELI Principles and Guidance*, principle 7 and guidance to principle 7.

⁴⁸ European Law Institute, *ELI Principles and Guidance*, principle 7, guidance to principle 7; Koller and Lehmann, *Digital Assets in Enforcement and Insolvency*.

⁴⁹ European Law Institute, *ELI Principles and Guidance*, principles 7–8; UNIDROIT, *Principles on Digital Assets and Private Law*, principle 6.

⁵⁰ Law no. 134/2010 on the Code of Civil Procedure, art. 781, art. 790, art. 793; European Law Institute, *ELI Principles and Guidance*, principle 8.

searching digital devices, systems and accounts be effective, but also sensitive to privacy, trade secrets and confidential information.⁵¹ They also contemplate expert assistance where needed. For Romanian law, the lesson is that effective enforcement against self-hosted wallets cannot rest on brute coercion alone; it requires a procedurally disciplined model of targeted disclosure, expert involvement and judicial supervision.

4.4. Preservation, Valuation and Sale of Self-Hosted Digital Assets

The preservation stage is where the limits of classical attachment become most visible. A formal seizure order has little practical value if the debtor can still move the asset in seconds from another device or through backup credentials. This is why Principle 8 of the ELI instrument insists that interim relief or comparable measures must be available to prevent dissipation before enforcement is completed.⁵²

In the self-hosted setting, preservation should be understood not merely as the physical seizure of a device, but as the secured neutralisation or migration of the debtor's digital asset position. The ELI Principles therefore recommend the availability of designated wallets under the authority of enforcement agents, used exclusively for assets resulting from enforcement and protected by appropriate cybersecurity measures.⁵³ This solution is conceptually superior to simple device seizure, because possession of a hardware wallet or laptop does not guarantee that the debtor lacks other backups or co-signing arrangements.

Valuation introduces a separate set of difficulties. Principle 10 of the ELI instrument emphasises that general valuation criteria and realisation methods must take account of volatility, the lack of pricing mechanisms and the absence of recognised markets.⁵⁴ Where a regulated or recognised market exists, market price at the date of enforcement may serve as the benchmark; where it does not, the enforcement authority should take reasonable steps to maximise the realisation value. The practical implication is that highly liquid crypto-assets, thinly traded tokens and non-fungible positions cannot be valued with the same procedural simplicity.

The same functional logic should govern sale. The ELI text envisages several routes, including transfer to the creditor at its request, forced judicial sale, sale through an approved exchange platform, public auction and direct agreement where that route better preserves value.⁵⁵ Under Romanian law, Article 793 of the

⁵¹ European Law Institute, *ELI Principles and Guidance*, principle 7 and guidance to principle 7.

⁵² European Law Institute, *ELI Principles and Guidance*, principle 8(3).

⁵³ European Law Institute, *ELI Principles and Guidance*, principle 9 and guidance to principle 9.

⁵⁴ European Law Institute, *ELI Principles and Guidance*, principle 10 and guidance to principle 10.

⁵⁵ European Law Institute, *ELI Principles and Guidance*, principle 10 and guidance to principle 10; Law no. 134/2010 on the Code of Civil Procedure, art. 793.

Code of Civil Procedure already provides that attachable securities and other intangible movables are realised according to the rules on movable enforcement, taking into account any special regime applicable to the asset. Once effective access to the self-hosted asset has actually been secured, that provision can support the realisation phase. The real bottleneck, however, lies earlier: without lawful and effective access, the ordinary rules on sale remain formally available but practically inert.

5. CASP Garnishment versus Self-Hosted Wallet Enforcement: A Functional Comparison

5.1. Intermediation as the True Criterion of Enforceability

The comparison developed in the preceding sections suggests that the decisive line in digital-asset enforcement is not the abstract opposition between “traditional” and “digital” assets, but the more precise distinction between intermediated control and direct control. Where a crypto-asset position is held with a CASP, the debtor’s relationship to the asset is translated into a legally intelligible intermediary relationship. That translation matters because Romanian garnishment law is structurally built around the presence of a third party who owes, holds, or administers attachable value in the debtor’s name. MiCA reinforces this legal readability by requiring authorisation, client-specific record keeping, position statements, segregation of client assets, and return procedures. In other words, a hosted crypto-asset position is not easier to enforce because it is less digital, but because it is more thoroughly institutionalised.⁵⁶

The self-hosted model reverses that structure. Regulation (EU) 2023/1113 recognises self-hosted addresses primarily at the point where they interact with CASPs, but it does not transform them into a standing institutional relationship comparable to a hosted account. Outside the regulated gateway, there is no professional intermediary who can routinely identify the client, segregate the relevant position, disclose the balance, and comply with a freezing order. As a result, enforcement must focus directly on the debtor’s power to control the asset through private credentials. In this setting, the language of control becomes more accurate than the language of possession, and the central legal question becomes whether the debtor can still operate the digital asset rather than whether a third party “holds” it in the classic sense.⁵⁷

For enforcement law, the hosted/self-hosted distinction is therefore not

⁵⁶ Law no. 134/2010 on the Code of Civil Procedure, art. 781(1), art. 784(1)–(4); Regulation (EU) 2023/1114, art. 59, art. 75(1), (5)–(8).

⁵⁷ Regulation (EU) 2023/1113, art. 3(20), art. 14(5), art. 16(2); UNIDROIT, *Principles on Digital Assets and Private Law*, principle 6 and commentary; European Law Institute, *ELI Principles and Guidance*, principle 8.

merely descriptive. It determines the object of attachment, the addressee of coercive measures, the kind of evidence available to the creditor, and the procedural sequence through which value may be preserved and realised. Hosted positions fit, albeit imperfectly, into a model of execution based on the legal compellability of an intermediary. Self-hosted positions reveal the limits of that model by concentrating effective power at debtor level. The practical consequence is that intermediation, rather than digitality as such, emerges as the true criterion of enforceability.⁵⁸

5.2. Evidentiary Asymmetry and Enforcement Efficiency

This structural distinction produces a profound evidentiary asymmetry. In the hosted environment, the most important elements of proof are generated and stored within the intermediary relationship itself: identity records, account architecture, custody logs, transaction history, balance information, operational freezes and internal references linking a client to specific positions. Once served with a garnishment order, the CASP is able, at least in principle, to confirm whether the debtor maintains relevant positions and to preserve them pending further enforcement steps. The hosted model thus transforms technical complexity into documentary and institutional traceability. Much of the evidentiary burden is effectively absorbed by the intermediary's own compliance and record-keeping architecture.⁵⁹

The self-hosted model is evidentially different in kind, not merely in degree. Here, the creditor must reconstruct control *ex post* from fragmented indicators: on-chain movements, historical transfers from known exchange accounts, device traces, communications, admissions, multisignature arrangements, or expert analysis. The EBA Travel Rule Guidelines are illuminating precisely because they show how difficult the notion of ownership or controllership of a self-hosted address is in practice. The methods they envisage — blockchain analytics, customer-provided information, minimal test transfers, digital signature checks, and combinations of technical means — demonstrate that proof of control is cumulative, situational and often probabilistic. These methods are useful, but they were designed for risk-based compliance at the gateway, not as automatic substitutes for judicial proof of present control in civil enforcement.⁶⁰

The divergence in enforcement efficiency follows directly from that evidentiary asymmetry. Hosted garnishment is comparatively front-loaded with legal compulsion: once the intermediary is identified and served, the system can

⁵⁸ Rodríguez de las Heras Ballell, "Emergence of Principles and Best Practices."

⁵⁹ Regulation (EU) 2023/1114, art. 75(5)–(8); Regulation (EU) 2023/1113, arts. 14–16; Law no. 134/2010 on the Code of Civil Procedure, arts. 783–784.

⁶⁰ European Banking Authority, *Travel Rule Guidelines*, paras. 77–86; Regulation (EU) 2023/1113, art. 14(5), art. 16(2).

move rapidly toward freezing, disclosure and, if needed, validation. Self-hosted enforcement is comparatively investigation-heavy and expert-dependent: it requires attribution, technical analysis, carefully framed access measures and constant attention to the risk of rapid dissipation. This is why recent European guidance places such strong emphasis on search measures, access to information and expert support when digital assets are held outside intermediary structures. From a functional perspective, the problem is not simply that self-hosted wallets are harder to “find,” but that the legal system cannot outsource factual complexity to a regulated third party.⁶¹

5.3. Debtor Protection, Proportionality and Privacy/Security Concerns

The comparative advantage of hosted enforcement does not eliminate the need for procedural restraint. Because CASPs hold extensive identity, transactional and sometimes behavioural data, any garnishment or disclosure measure directed to them must remain confined to what is necessary for the enforcement purpose pursued. The relevant balance is not exhausted by creditor effectiveness. It also engages the debtor’s right to property, the right to an effective remedy, and the rights to privacy and data protection under the Charter of Fundamental Rights of the European Union. In the hosted context, proportionality therefore requires targeted identification of the relevant account relationship, limited disclosure of what is actually needed for the enforcement file, and secure handling of the data generated through compliance with the order.⁶²

Those concerns become even sharper in the self-hosted environment. Measures aimed at identifying or neutralising debtor-controlled wallets may require access to devices, backup systems, address books, seed phrases, or other credentials that potentially unlock far more than the specific asset targeted by the creditor. An overbroad order may reveal unrelated holdings, third-party relationships, commercial secrets or personal data far beyond the scope of the enforcement file. It may also create cybersecurity risks by forcing the disclosure, duplication or insecure storage of access credentials. For that reason, self-hosted enforcement cannot be conceived merely as a more intrusive version of hosted gar-

⁶¹ European Law Institute, *ELI Principles and Guidance*, principles 7–8, and guidance to principles 7–8.

⁶² Charter of Fundamental Rights of the European Union, *Official Journal of the European Union* C 326 (October 26, 2012): 391–407, art. 7, art. 8, art. 17, art. 47, https://eur-lex.europa.eu/eli/treaty/char_2012/oj/eng; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union* L 119 (May 4, 2016): 1–88, art. 5(1)(b), (c), (f), art. 6(1)(c), art. 32, <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>.

nishment. It is a distinct category of intervention requiring tighter judicial supervision and much more rigorous tailoring of the measures employed.⁶³

Accordingly, proportionality should operate as the common metric governing both models, but with different practical consequences in each. In hosted enforcement, proportionality points toward calibrated freezing and disclosure duties imposed on the CASP. In self-hosted enforcement, it points toward a staged approach: first, targeted identification; second, carefully limited access measures; third, expert-supervised transfer or preservation; and only thereafter valuation and sale. The ELI Principles are especially persuasive on this point because they recommend mechanisms such as designated enforcement wallets and secure preservation procedures, thereby reducing the need for uncontrolled exposure of debtor credentials while still making enforcement effective. This approach does not weaken creditor protection; on the contrary, it increases the legitimacy, operational safety and judicial defensibility of enforcement measures in a field where overreach may easily render execution both contestable and technically fragile.⁶⁴

The comparison therefore confirms the central thesis of the article. The decisive predictor of enforceability in the digital-asset environment is not whether the asset is recorded on a blockchain, but whether control over that asset has been externalised into a legally reachable intermediary relationship or remains concentrated in the debtor's own technical sphere. Once that distinction is accepted, the apparent diversity of execution problems becomes analytically clearer: hosted accounts primarily test the adaptability of classical garnishment, while self-hosted wallets expose the need for more explicit procedural tools, stronger proportionality controls and technically informed enforcement design.⁶⁵

6. *De Lege Lata* and *De Lege Ferenda* Observations

6.1. What Current Romanian Law Already Allows

Romanian law already provides a meaningful, although incomplete, basis for enforcement against digital assets. The decisive point is that the Code of Civil Procedure does not confine garnishment to bank deposits or narrowly defined receivables. Article 781 of the Code of Civil Procedure extends garnishment to sums of money, securities, and other attachable intangible movable assets owed to the debtor or held in the debtor's name by a third party. Read together

⁶³ European Law Institute, *ELI Principles and Guidance*, principles 7–9; UNIDROIT, *Principles on Digital Assets and Private Law*, principle 6 and commentary.

⁶⁴ Charter of Fundamental Rights of the European Union, art. 47, art. 52(1); European Law Institute, *ELI Principles and Guidance*, principles 8–10; Law no. 134/2010 on the Code of Civil Procedure, art. 793.

⁶⁵ Rodríguez de las Heras Ballell, “Emergence of Principles and Best Practices”; Lehmann, “Who Owns Bitcoin?”

with the ELI view that general enforcement provisions should apply to digital assets to the greatest extent possible and that digital-specific rules should be reserved for cases where they are truly necessary, the better *de lege lata* conclusion is that the absence of an express statutory reference to crypto-assets does not, by itself, exclude them from enforcement. It rather requires a functionally informed application of existing categories.⁶⁶

That conclusion is strongest in relation to crypto-assets held through a CASP. Romanian law already contains the operative sequence needed for hosted positions: garnishment is created without prior summons; service on the third party triggers immediate unavailability of the attached position; the third-party garnishee must preserve the attachable intangible assets and prove compliance; validation proceedings are available if the garnishee fails to comply; and, where the garnishment concerns securities or other intangible movables, Article 793 of the Code of Civil Procedure authorises their realisation under the rules governing movable enforcement. MiCA substantially reinforces the feasibility of this reading because Article 75 requires custody providers to keep client-specific registers of positions, issue statements of position, maintain return procedures, and segregate client assets from the provider's own estate. In practical terms, MiCA supplies the informational and operational architecture that classical Romanian garnishment needs in order to function effectively against hosted crypto-asset positions.⁶⁷

Romanian law also already offers a conservatory layer that can be adapted to digital assets. Articles 952 and 953 CPC allow conservatory seizure where the creditor does not yet hold an enforceable title but can show a due claim, a pending action, or a risk that the debtor will dissipate assets. In addition, Article 783(7) of the Code of Civil Procedure contemplates the continuation of a garnishment initially established as a security measure once the creditor obtains an enforceable title. For volatile digital assets, especially where a reachable intermediary exists, this matters greatly: it allows value to be immobilised before transferability and price instability deprive the future enforcement of practical utility.⁶⁸

What current Romanian law does not provide is a self-standing procedural toolkit for assets held in self-custody. Even so, it would be inaccurate to conclude that the law is entirely powerless. Article 790(3) of the Code of Civil Procedure already permits the taking of any evidence admissible under ordinary

⁶⁶ Law no. 134/2010 on the Code of Civil Procedure, art. 781(1); European Law Institute, *ELI Principles and Guidance*, principle 2 and guidance to principle 2; Rodríguez de las Heras Ballell, "Emergence of Principles and Best Practices."

⁶⁷ Law no. 134/2010 on the Code of Civil Procedure, art. 783(1)–(2), art. 784(1)–(4), art. 787(1), (3), (5), art. 790(1)–(9), art. 792(1)–(2), art. 793; Regulation (EU) 2023/1114, art. 75(2)–(8); Zetzsche and Woxholth, *EU Law on Crypto-Assets*.

⁶⁸ Law no. 134/2010 on the Code of Civil Procedure, art. 783(7), art. 952, art. 953.

law in validation proceedings, and nothing in Romanian procedural law excludes expert evidence, device examination, transaction tracing, or the use of intermediary-generated records when the court must determine whether a relevant digital asset exists and whether it can be reached. Once this evidentiary openness is read alongside the UNIDROIT notion of control and the ELI emphasis on disclosure, search measures, and access to digital assets, current Romanian law can be understood as containing a partial interpretive basis for acting against self-hosted positions where identification and lawful access have already been achieved. The present weakness is therefore not a total absence of legal tools, but the lack of express procedural design for debtor-controlled digital assets.⁶⁹

6.2. What Romanian Law Should Clarify or Add

The first legislative step should not be the creation of a wholly separate enforcement code for crypto-assets. A better solution would be a targeted clarification in the Code of Civil Procedure stating that digital assets, including crypto-assets and other electronically recorded values capable of control, may constitute attachable assets or attachable intangible movable assets for enforcement purposes. This would be consistent with the ELI position that general enforcement rules should continue to apply as far as feasible, while specific rules should be introduced only where the functional, operational, or substantive characteristics of digital assets make them unavoidable. In a procedural system where analogy may be contested or applied cautiously, such an express clarification would improve certainty without sacrificing technological neutrality.⁷⁰

Second, Romanian law should introduce explicit disclosure duties tailored to digital assets. The debtor should be placed under a clear statutory obligation to disclose relevant CASP accounts, self-hosted wallets, recovery arrangements, multisignature participation, custodial relationships, and materially relevant prior transfers. The same framework should empower courts or enforcement agents, subject to appropriate procedural safeguards, to obtain information from relevant third parties, including CASPs and other service providers that can identify or trace the debtor's digital positions. ELI Principle 6 is especially persuasive here: it places a primary cooperation duty on the debtor, allows measures compelling disclosure, envisages recourse to third parties where the debtor does not cooperate, and calls for adequate and proportionate consequences for unjustified refusal or for false or misleading information. Romanian procedural law should

⁶⁹ Law no. 134/2010 on the Code of Civil Procedure, art. 790(3); UNIDROIT, *Principles on Digital Assets and Private Law*, principle 6 and commentary; Lehmann, "Who Owns Bitcoin?"; European Law Institute, *ELI Principles and Guidance*, principles 6–8; Koller and Lehmann, *Digital Assets in Enforcement and Insolvency*.

⁷⁰ European Law Institute, *ELI Principles and Guidance*, principle 2 and guidance to principle 2; Law no. 134/2010 on the Code of Civil Procedure, art. 781(1).

move in precisely that direction.⁷¹

Third, the Code of Civil Procedure should contain a distinct regime for access measures directed at debtor-controlled wallets. Such a regime should authorise targeted search of relevant devices, systems, or accounts only where necessary and proportionate, and with preference for the least invasive measure capable of making enforcement effective. ELI Principles 4, 7, and 8 are particularly useful in this regard: they require proportionality, emphasise effective but privacy-sensitive search measures, and define access to digital assets in terms of actual attachment and effective seizure. The domestic implication is straightforward. Romanian law should move toward a staged procedural model: targeted identification first, narrowly tailored access measures second, secure transfer or neutralisation third, and only thereafter valuation and sale. Broad or undefined orders requiring indiscriminate disclosure of all credentials would be difficult to reconcile with proportionality and should therefore be avoided.⁷²

Fourth, Romanian law should create a secure custody infrastructure for assets that have already been seized. The most convincing solution is a designated enforcement wallet, or an equivalent secure technical arrangement, used exclusively for preservation and transfer within enforcement proceedings. ELI Principle 9 expressly recommends the implementation of technological solutions enabling seizure and appropriate custody, including designated wallets under the authority of enforcement agents. MiCA's custody framework points in the same direction at the level of regulatory technique: it emphasises registers of positions, segregation, and secure handling of access means. A Romanian designated-wallet mechanism would not replicate MiCA, but it would draw from the same operational insight, namely that seizure is ineffective if the legal system cannot also guarantee secure post-seizure custody.⁷³

Fifth, Romanian law should set clearer valuation and realisation rules for digital assets. Article 793 of the Code of Civil Procedure already allows the sale of securities and other intangible movables under the rules governing movable enforcement, but digital assets require more detailed guidance on timing, method, and market selection. ELI Principle 10 expressly recommends that valuation and realisation should take account of volatility, the lack of pricing mechanisms, and the possible absence of recognised markets, while the chosen method should aim to maximise value and minimise unnecessary market impact. A domestic rule could therefore combine a duty-of-care standard with expressly recognised routes such as sale through a suitably regulated platform, judicial sale, transfer in kind to the creditor where lawful and requested, or another method appropriate to the

⁷¹ European Law Institute, *ELI Principles and Guidance*, principle 6 and guidance to principle 6.

⁷² European Law Institute, *ELI Principles and Guidance*, principle 4, principles 7–8 and accompanying guidance.

⁷³ European Law Institute, *ELI Principles and Guidance*, principle 9 and guidance to principle 9; Regulation (EU) 2023/1114, art. 75(2)–(8).

subclass of asset involved.⁷⁴

Finally, reform should address the cross-border dimension of digital-asset enforcement. ELI Principle 3 highlights the need for clearer and more harmonised rules on applicable law, jurisdiction, and access across jurisdictions, while the guidance to Principle 6 warns that tying cooperation duties to the residence or establishment of the debtor or third party may create serious inefficiencies in multi-jurisdictional cases. Romanian law cannot solve that problem on its own, but it can reduce friction by clarifying who may be served, what foreign-facing intermediaries must disclose when a Romanian enforcement proceeding is pending, and how courts should structure cooperation requests concerning digital assets that are controlled or evidenced abroad. In a market defined by technological delocalisation, procedural clarity about cooperation is not ancillary; it is a precondition of effectiveness.⁷⁵

7. Conclusions

This article has argued that the decisive criterion of enforceability in the field of crypto-assets is not digitality as such, but the legal architecture through which control over value is exercised. Where the debtor's position is maintained through a crypto-asset service provider, Romanian civil procedure can, in principle, adapt the classical logic of garnishment because there is an identifiable intermediary capable of being served, compelled to freeze the relevant position, and required to preserve and disclose attachable value. In this setting, MiCA does not itself create a special enforcement regime, but it significantly strengthens the operational viability of garnishment by requiring client-specific records, segregation, return procedures, and continuity arrangements. The hosted model is therefore not fully assimilable to a bank account, yet it is sufficiently institutionalised to fit within the existing framework of attachment of intangible movable assets held by a third party.⁷⁶

By contrast, self-hosted wallets reveal the structural limits of an enforcement model historically built around physical location or institutional intermediation. In the absence of a garnishee, the decisive questions become attribution, proof of present control, lawful access, secure preservation, and technically appropriate realisation. This is why the concept of control is more analytically use-

⁷⁴ Law no. 134/2010 on the Code of Civil Procedure, art. 793; European Law Institute, *ELI Principles and Guidance*, principle 10 and guidance to principle 10.

⁷⁵ European Law Institute, *ELI Principles and Guidance*, principle 3, principle 6 and accompanying guidance; Rodríguez de las Heras Ballell, "Emergence of Principles and Best Practices."

⁷⁶ Law no. 134/2010 on the Code of Civil Procedure, art. 781(1), art. 783–784, art. 790–793; Regulation (EU) 2023/1114, art. 75(2)–(8); Rodríguez de las Heras Ballell, "Emergence of Principles and Best Practices."

ful than the inherited language of possession. A self-hosted digital asset is enforceable only to the extent that the legal system can identify the relevant position, demonstrate that the debtor still controls it, and transform that control into an effective and proportionate seizure mechanism. Existing Romanian law offers fragments of this architecture through general evidentiary openness and movable-enforcement rules, but it does not yet provide a sufficiently explicit procedural design for debtor-controlled digital assets.⁷⁷

The comparison between hosted and self-hosted models also demonstrates a marked evidentiary asymmetry. Hosted enforcement benefits from the documentary and operational infrastructure of the intermediary, which concentrates identity, transaction history, balance information, and freezing capacity in a legally reachable entity. Self-hosted enforcement, by contrast, remains investigation-heavy, expert-dependent, and acutely vulnerable to rapid dissipation of value. At the same time, the search for effectiveness cannot justify procedurally unbounded interference. The more enforcement depends on access to credentials, devices, or other technically sensitive elements, the stronger the need for proportionality, privacy protection, cybersecurity safeguards, and judicial supervision.⁷⁸

The practical implication is that Romanian law should not abandon its general enforcement framework, but refine it. The preferable path is a targeted reform agenda: express recognition that digital assets may constitute attachable intangible movable assets; clearer debtor and third-party disclosure duties; tailored rules on search and access measures; secure post-seizure custody solutions such as designated enforcement wallets; and more precise standards on valuation and realisation in conditions of volatility and fragmented market structure. Such adjustments would not amount to a rupture with the Code of Civil Procedure. They would instead represent a technologically informed continuation of its underlying logic.⁷⁹

The broader result of the study is therefore twofold. First, Romanian law already contains a plausible *de lege lata* basis for enforcement against crypto-assets held with CASPs. Second, self-hosted wallets expose a genuine procedural gap that cannot be satisfactorily addressed by simple analogy with bank-account garnishment. In the digital-asset environment, the future of enforcement law depends on its ability to move from categories designed for physical control or institutional custody toward rules capable of addressing digitally mediated control

⁷⁷ UNIDROIT, *Principles on Digital Assets and Private Law*, principle 6 and commentary; European Law Institute, *ELI Principles and Guidance*, principles 7–10; Lehmann, “Who Owns Bitcoin?”

⁷⁸ Charter of Fundamental Rights of the European Union, art. 7, art. 8, art. 17, art. 47, art. 52(1); Regulation (EU) 2016/679, art. 5(1)(b), (c), (f), art. 6(1)(c), art. 32; European Law Institute, *ELI Principles and Guidance*, principle 4, principles 7–8.

⁷⁹ European Law Institute, *ELI Principles and Guidance*, principle 2, principle 6, principle 7, principle 9, principle 10 and accompanying guidance; Law no. 134/2010 on the Code of Civil Procedure, art. 781, art. 790, art. 793.

without sacrificing legal certainty, proportionality, or procedural fairness.⁸⁰

Bibliography

I. Doctrinal Sources

1. Brummer, Chris, ed. *Cryptoassets: Legal, Regulatory, and Monetary Perspectives*. New York: Oxford University Press, 2019. <https://doi.org/10.1093/oso/9780190077310.001.0001>.
2. De Filippi, Primavera, and Aaron Wright. *Blockchain and the Law: The Rule of Code*. Cambridge, MA: Harvard University Press, 2018. <https://doi.org/10.4159/9780674985933>.
3. Gullifer, Louise, and Ignacio Tirado. "Proprietary Rights and Digital Assets: A 'Modest Proposal' from a Transnational Law Perspective." *Law and Contemporary Problems* 87, no. 2 (2025): 211–232. <https://scholarship.law.duke.edu/lcp/vol87/iss2/9/>.
4. Koller, Christian, and Matthias Lehmann, eds. *Digital Assets in Enforcement and Insolvency: Securing Creditor Access and Protecting Customer Interests in the Crypto World*. Oxford: Hart Publishing, 2025. <https://doi.org/10.5040/9781509976782>.
5. Lehmann, Matthias. "Who Owns Bitcoin? Private Law Facing the Blockchain." *Minnesota Journal of Law, Science & Technology* 21, no. 1 (2020): 93–136. <https://doi.org/10.24926/15529541.3823>.
6. Rodríguez de las Heras Ballell, Teresa. "The Emergence of Principles and Best Practices on Digital Assets: Proprietary Rights, and Enforcement." *European Journal of Risk Regulation*, published online October 4, 2024, 1–12. <https://doi.org/10.1017/err.2024.55>.
7. Veneziano, Anna, and Teresa Rodríguez de las Heras Ballell. "Digital Assets in Insolvency and Enforcement Proceedings: Some Insights from UNIDROIT's Work." In *Digital Assets in Enforcement and Insolvency: Securing Creditor Access and Protecting Customer Interests in the Crypto World*, edited by Christian Koller and Matthias Lehmann, 27–43. Oxford: Hart Publishing, 2025. <https://doi.org/10.5040/9781509976782>.
8. Werbach, Kevin. *The Blockchain and the New Architecture of Trust*. Cambridge, MA: MIT Press, 2018. <https://doi.org/10.7551/mitpress/11449.001.0001>.
9. Zetzsche, Dirk, and Jannik Woxholth. *The EU Law on Crypto-Assets: A Guide to European FinTech Regulation*. Cambridge: Cambridge University Press, 2025. <https://doi.org/10.1017/9781009196338>.
10. Zetzsche, Dirk, and Jannik Woxholth. "Crypto Custody." In *The EU Law on Crypto-Assets: A Guide to European FinTech Regulation*, 130–143. Cambridge:

⁸⁰ Koller and Lehmann, *Digital Assets in Enforcement and Insolvency*; Veneziano and Rodríguez de las Heras Ballell, "Digital Assets in Insolvency and Enforcement Proceedings"; Regulation (EU) 2023/1114, art. 61, art. 65; European Law Institute, *ELI Principles and Guidance*, principle 3 and guidance to principle 3; Rodríguez de las Heras Ballell, "Emergence of Principles and Best Practices."

Cambridge University Press, 2025. <https://doi.org/10.1017/9781009196338.010>.

11. Zetzsche, Dirk, and Jannik Woxholth. "Private Law of Cryptoassets." In *The EU Law on Crypto-Assets: A Guide to European FinTech Regulation*, 203–216. Cambridge: Cambridge University Press, 2025. <https://doi.org/10.1017/9781009196338.015>.

II. Legislation and Soft-Law Instruments

1. Charter of Fundamental Rights of the European Union. *Official Journal of the European Union* C 326 (October 26, 2012): 391–407. https://eur-lex.europa.eu/eli/treaty/char_2012/oj/eng.
2. European Banking Authority. *Guidelines on Information Requirements in Relation to Transfers of Funds and Certain Crypto-Assets Transfers under Regulation (EU) 2023/1113 (Travel Rule Guidelines)*. EBA/GL/2024/11. July 4, 2024. <https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-counteracting-financing-terrorism/guidelines-information-requirements-relation-transfers-funds-and-certain-crypto-assets-transfers>.
3. European Law Institute. *ELI Principles and Guidance for Enforcement Against Digital Assets*. Vienna: European Law Institute, 2025. https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Projects/Access_to_Digital_Assets/ELI_Principles_and_Guidance_for_Enforcement_Against_Digital_Assets.pdf.
4. Romania. *Legea nr. 134/2010 privind Codul de procedură civilă* [Law no. 134/2010 on the Code of Civil Procedure]. Republished in *Monitorul Oficial al României*, Part I, no. 247, April 10, 2015, as subsequently amended. <https://legislatie.just.ro/Public/DetaliuDocument/140271>.
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* L 119 (May 4, 2016): 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>.
6. Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849. *Official Journal of the European Union* L 150 (June 9, 2023): 1–39. <https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng>.
7. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No. 1093/2010 and (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. *Official Journal of the European Union* L 150 (June 9, 2023): 40–205. <https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng>.
8. UNIDROIT. *Principles on Digital Assets and Private Law*. Rome: UNIDROIT, 2023. <https://www.unidroit.org/work-in-progress/digital-assets-and-private-law>.